ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 104 (2004) 287–300

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Determining L-functions by twists

H. Kisilevsky[1]

Department of Mathematics and Statistics and CICMA Concordia University, 1455 de Maisonneuve Blvd. West Montréal, Quebec, Canada H3G 1M8

Received 5 February 2003; revised 6 May 2003

Communicated by D. Goss

Abstract

Suppose that $L_1(s)$ and $L_2(s)$ are two L-functions whose twists by a set of Dirichlet characters simultaneously vanish (vanish mod p) at a critical point. We examine the extent to which this property determines the L-functions in the cases of L-functions of elliptic curves, of number fields, and of curves over finite fields.

1. Introduction

There has been considerable interest in the study of special values of twists of L-functions (and their derivatives) by Hecke characters. The vanishing or non-vanishing of such values have profound arithmetic significance, especially when twisting by Dirichlet characters.

In this article, we investigate the following question: Is an L-function, $L(s)$, characterized by the set of Dirichlet characters for which the corresponding twisted L-function vanishes at a critical point (or vanishes modulo a set of primes in a suitable sense)? We consider three classes of L-functions: Dirichlet L-functions, L-functions of abelian varieties over finite fields, and L-functions associated to modular forms.

In Section 2, we consider the vanishing of the central values of twists of modular L-functions by quadratic Dirichlet characters. In Section 3, we study Dirichlet L-functions and in Section 4 the L-functions of curves over finite fields. In the latter

E-mail address: kisilev@mathstat.concordia.ca.

[1] This work was supported in part by grants from NSERC and FCAR.

0022-314X/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S0022-314X(03)00158-6

two cases, the L-functions do not vanish, and we consider instead the vanishing modulo primes of an "algebraic part" defined below.

This question is related to a conjecture of Y. Zarhin. Zarhin's conjecture asserts that: If X_1 and X_2 are two abelian varieties defined over a number field k, with the property that

$$\mathrm{rank}_{\mathbb{Z}}(X_1(K)) = \mathrm{rank}_{\mathbb{Z}}(X_2(K))$$

for all finite extensions K/k, then X_1 and X_2 are isogenous over k. (Here, by $\mathrm{rank}_{\mathbb{Z}}(X(K))$ we mean the number of free generators of the Mordell–Weil group $X(K)$.)

In view of Faltings' theorem the analytic form of this conjecture is the statement: If

$$\mathrm{ord}_{s=1}L(X_1/K,s) = \mathrm{ord}_{s=1}L(X_2/K,s)$$

for all finite extensions K/k, then

$$L(X_1/k,s) = L(X_2/k,s),$$

where $L(X_i/K,s)$ is the L-function of X_i viewed as a variety over K. Restricting to *abelian* extensions one may modify the conjecture as follows: If

$$\mathrm{ord}_{s=1}L(X_1/k,s,\chi) = \mathrm{ord}_{s=1}L(X_2/k,s,\chi)$$

for all (Hecke) characters χ of finite order, then

$$L(X_1/k,s) = L(X_2/k,s),$$

where $L(X_i/k,s,\chi)$ is the L-function of X_i/k twisted by the character χ.

The work of Rohrlich [Ro] provides a corresponding (conjectural) algebraic interpretation in terms of the ranks of the "χ-components" of the Mordell–Weil groups $X_i(k^{\mathrm{ab}})$. Specifically, if X is an abelian variety defined over k, then $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ acts on $X(k^{\mathrm{ab}})$. If we set $V = \mathbb{C}\otimes_{\mathbb{Z}}X(k^{\mathrm{ab}})$, then V is a representation space for $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ and decomposes $V = \oplus_{\chi}V(\chi)$ into finite dimensional eigenspaces $V(\chi)$ on which $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ acts via the character χ. On the other hand, to each such character of $\mathrm{Gal}(k^{\mathrm{ab}}/k)$, one associates the L-function, $L(X/k,s,\chi)$, afforded by the tensor product of χ with the ℓ-adic representation of X. Rohrlich then shows, that the Birch and Swinnerton-Dyer conjecture together with the Deligne–Gross conjecture imply that

$$\dim_{\mathbb{C}} V(\chi) = \mathrm{ord}_{s=1}L(X/k,s,\chi).$$

The analytic conjectures have the advantage that they can be asked for a wider class of L-functions and that they have analogues even in the case of non-vanishing.

In [Ki] we considered Zarhin's conjecture in the case of elliptic curves defined over $\mathbb{Q}$, and proved the following two statements:

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ such that

$$\mathrm{ord}_{s=1}L(E_1/K,s) \equiv \mathrm{ord}_{s=1}L(E_2/K,s) \pmod 2$$

for all extensions $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \leqslant 2$, then $N(E_1)$ and $N(E_2)$ are equal up to square factors (where $N(E)$ is the conductor of E). In particular, if E_1 and E_2 are semi-stable, then there are only finitely many isogeny classes of such curves.

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ such that

$$\mathrm{rank}_{\mathbb{Z}}(E_1(K)) \equiv \mathrm{rank}_{\mathbb{Z}}(E_2(K)) \pmod 2$$

for all extensions $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \leqslant 2$ and suppose that the 2-primary part of their Tate–Shafarevich groups, $Ш(E_i(K))_2$, are finite for all such K, then $N(E_1)$ and $N(E_2)$ are equal up to square factors.

2. Elliptic curves and modular L-functions

Let E be an elliptic curve defined over $\mathbb{Q}$. We denote the L-function of $E/\mathbb{Q}$ by $L(E/\mathbb{Q},s) = L(E,s)$, and denote its twist by the Dirichlet character χ by $L_\chi(E,s) = L(E,s,\chi)$.

Theorem 2.1. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ such that*

$$L(E_1,1,\chi) = 0 \Leftrightarrow L(E_2,1,\chi) = 0$$

for every quadratic Dirichlet character χ. Then their conductors, $N(E_1)$ and $N(E_2)$, are equal up to square factors.

Proof. The elliptic curves E_1 and E_2 are modular by the recent work of Wiles and Taylor–Wiles, and Breuil–Conrad–Diamond–Taylor [Wi,Ta–Wi,B–C–D–Ta]. Their L-functions have an analytic continuation to the entire plane, and that they satisfy a functional equation. Applying Waldspurger's result [Wa], we see that there exists a quadratic character χ_1 of conductor D_1 prime to $N(E_1)$ and $N(E_2)$, such that the twisted L-function $L(E_1,1,\chi_1) \neq 0$. The hypothesis then implies that $L(E_2,1,\chi_1) \neq 0$ and so the L-functions $L(E_i,s,\chi_1)$ both have $+1$ as signs in their functional equations and conductors $N(E_1)D_1^2$ and $N(E_2)D_1^2$ respectively. If $N(E_1)$ and $N(E_2)$, were not equal up to square factors, there would exist a prime p which appears in the factorization of $N(E_1)$ (say) to an *odd* power and to an *even* power in $N(E_2)$. Using the extension of Waldspurger's theorem of Friedberg–Hoffstein [Fr–Ho], we can choose a character χ_2 of conductor D_2 prime to $N(E_1)$, $N(E_2)$ and D_1 which satisfies: $\chi_2(l) = 1$ for all primes $l \neq p$ dividing $N(E_1)N(E_2)D_1$; and such that $\chi_2(-1) = +1$, $\chi_2(p) = -1$ and for which $L(E_2,1,\chi_1 \cdot \chi_2) \neq 0$. This exists as the sign of the functional equation for $L(E_2,s,\chi_1 \cdot \chi_2)$ is $\chi_2(-N(E_2)D_1^2) = +1$ times that of $L(E_2,s,\chi_1)$ and hence is $+1$. Then the sign of the functional equation of $L(E_1,s,\chi_1 \cdot \chi_2)$ is

$\chi_2(-N(E_1)D_1^2)$ times that of $L(E_1,s,\chi_1)$ and hence is -1. But this implies that $L(E_1,1,\chi_1\cdot\chi_2)=0$ contradicting the hypothesis of Theorem 2.1. □

Virtually the same argument will carry over to the case of L-functions attached to normalized newforms of weight $2k$ for $\Gamma_0(M)$.

Theorem 2.2. *Suppose that $f_i\in S_{2k}(M_i,\chi_0)$, $i=1,2$, are normalized newforms of weight $2k$, and trivial nebentypus. Let $L(s,f_i)$ be their associated L-functions. Suppose that*

$$L_\chi(k,f_1)=0\Leftrightarrow L_\chi(k,f_2)=0$$

for all quadratic Dirichlet characters, χ. Then M_1 and M_2 are equal up to square factors.

Proof. Let $\Lambda(s,f_i)=\left(\sqrt{M_i}/2\pi\right)^s\Gamma(s)L(s,f_i)$. For χ a quadratic Dirichlet character of conductor D_χ relatively prime to M_i, let

$$\Lambda_\chi(s,f_i)=\left(D_\chi\sqrt{M_i}/2\pi\right)^s\Gamma(s)L_\chi(s,f_i).$$

Then, since we have assumed that f_i is a normalized newform, we have $f_i=\overline{f_i}$, and since χ is a quadratic character, it follows (see [Mi, Section 4.3] or [Sh, Theorem 3.66]), that the twist, $f_{i,\chi}$, of f_i belongs to $S_{2k}(M_iD_\chi^2,\chi_0)$, and that $\Lambda_\chi(s,f_i)$ satisfies the functional equation

$$\Lambda_\chi(2k-s,f_i)=\varepsilon_\chi\Lambda_\chi(s,f_i)$$

with $\varepsilon_\chi=\pm1$. Furthermore, since the conductor D_χ of χ is relatively prime to M_i, it follows that $\varepsilon_\chi=\chi(-M_i)\varepsilon$, where ε is the sign of the functional equation for $\Lambda(s,f_i)$. The rest of the argument proceeds as in the proof of Theorem 2.1. □

Remark. The Friedberg–Hoffstein result has been further strengthened by Ono–Skinner [O–Sk2, Corollary 3]). They show that among all quadratic twists (with conductors divisible by exactly k primes, and satisfying finitely many local sign conditions) of an L-function associated to a newform, a *positive proportion* will not vanish at the centre of the critical strip.

Corollary 2.3. *Let E_1 and E_2 be semi-stable elliptic curves defined over $\mathbb{Q}$ such that*

$$L(E_1,1,\chi)=0\Leftrightarrow L(E_2,1,\chi)=0$$

for every quadratic Dirichlet character χ. Then their conductors, $N(E_1)$ and $N(E_2)$, are equal.

Proof. By Theorem 2.1, $N(E_1) = N(E_2)$ up to square factors. Since E_1 and E_2 be semi-stable, they have square-free conductors, so it follows that $N(E_1) = N(E_2)$. □

3. Dirichlet L-functions

Let ψ be a primitive quadratic (Dirichlet) character of conductor N_ψ. Let $K(= \mathbb{Q}(\psi))$ be the quadratic field corresponding to ψ. Then $K = \mathbb{Q}\left(\sqrt{D_\psi}\right)$ where $D_\psi = \psi(-1)N_\psi$ is the discriminant of K, and $L(s) = L(s,\psi)$ is the Dirichlet L-function associated to K. Then if ψ is not the trivial character χ_0, we have $L(1,\psi) \neq 0$, and we let the "algebraic part" $L^*(1,\psi)$ of $L(1,\psi)$ be the class number $h(K)(= h(\psi) = h(D_\psi))$ of K. The trivial character corresponds to $\mathbb{Q}(\chi_0) = \mathbb{Q}$, and $L^*(1,\chi_0) = 1$. For another quadratic character χ, the "twist" $L_\chi(s,\psi) = L(s,\psi\cdot\chi)$ of $L(s,\psi)$ is the Dirichlet L-function associated to the *primitive* quadratic character $\psi\cdot\chi$. Denote by $K(\chi)(= \mathbb{Q}(\psi\cdot\chi))$ the extension of $\mathbb{Q}$ corresponding to the primitive Dirichlet character $\psi\cdot\chi$. Then $K(\chi) = \mathbb{Q}\left(\sqrt{D_\psi D_\chi}\right)$ and $L^*(1,\psi\cdot\chi)$ is the class number $h(\mathbb{Q}(\psi\cdot\chi)) = h(K(\chi))$.

Suppose now that L_1 and L_2 are Dirichlet L-functions, for the quadratic characters ψ_1 and ψ_2 respectively. Let $K_1\left(= \mathbb{Q}\left(\sqrt{D_1}\right)\right)$ and $K_2\left(= \mathbb{Q}\left(\sqrt{D_2}\right)\right)$ be the associated quadratic fields. Suppose that L_1 and L_2 satisfy the following: There is a set S of primes such that for all $p\in S$ and for all quadratic Dirichlet characters χ (including the trivial character χ_0), we have

$$L^*(1,\psi_1\cdot\chi) \equiv 0 \pmod{p} \Leftrightarrow L^*(1,\psi_2\cdot\chi) \equiv 0 \pmod{p}.$$

Note that $2\in S$ implies that $h(K_1(\chi))$ is odd if and only if $h(K_2(\chi))$ is odd. We show below that if $2\in S$, then $L_1 = L_2$.

Theorem 3.1. *Let K_1 and K_2 be quadratic number fields such that, for all quadratic Dirichlet characters χ, the class number $h(K_1(\chi))$ is odd if and only if $h(K_2(\chi))$ is odd. Then $K_1 = K_2$.*

Proof. This follows from the Gauss' genus theory for quadratic fields.

We note that for an imaginary quadratic field, F, the class number $h(F)$ is odd if and only if the conductor $N(F)$ of F is a prime power, and for F a real quadratic field, $h(F)$ is odd if and only if either the conductor $N(F)$ is a prime power, or $N(F)$ is a product of two distinct prime powers, at least one of which is congruent to 3 (mod 4) (cf. [Na, Theorem 8.8 and Remark 20, p. 483]).

As above, we write $K_i = \mathbb{Q}\left(\sqrt{D_i}\right)$ for $i = 1, 2$. Since twisting both K_1 and K_2 by any quadratic character doesn't disturb the hypotheses, we can assume that $K_1 = \mathbb{Q}$.

Since $K_1 = \mathbb{Q}$ and $h(K_1) = 1$ is odd, the hypothesis implies that $h(K_2)$ is also odd. If $K_2 \neq K_1$, then we must have either $K_2 = \mathbb{Q}\left(\sqrt{-1}\right)$ or $\mathbb{Q}\left(\sqrt{-p}\right)$ with p a prime and

$p \equiv 2,3 \pmod 4$, if K_2 is an imaginary quadratic field, or $K_2 = \mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{p_1 p_2})$ with p, p_1, p_2 prime and at least one of $p_1, p_2 \equiv \pmod 4$. Choosing a prime $l \neq p, p_1, p_2$ with $l \equiv 1 \pmod 4$ and twisting by the real quadratic character χ corresponding to the field $\mathbb{Q}(\sqrt{l})$ we have $K_1(\chi) = \mathbb{Q}(\sqrt{l})$ and $h(K_1(\chi))$ is odd. But then $K_2 \neq K_1$ as above implies that $h(K_2(\chi))$ is even. It then follows that $K_1 = K_2$. □

The case that $2 \notin S$ poses interesting questions. In particular, consider the case that $S = \{p\}$ consists of a single *odd* prime p. For a fixed quadratic field K, one knows [Ha,Jo,O–Sk] that there are an infinite number of quadratic twists $K(\chi)$, of K, for which p does *not* divide the class number $h(K(\chi))$. It is an old result [An–Ch] that there are also an infinite number of quadratic twists $K(\chi')$, of K, for which p does divide the class number $h(K(\chi'))$.

Given two quadratic fields K_1, and K_2, it is not known whether one can find a common quadratic twist χ such that p divides $h(K_1(\chi))$ but does not divide $h(K_2(\chi))$.

Specifically, suppose that p is a fixed odd prime. If $K_i = \mathbb{Q}(\sqrt{-D_i})$ are distinct imaginary quadratic fields, does there exist an integer N such that the class number of $\mathbb{Q}(\sqrt{-D_1 N})$ is divisible by p, while the class number of $\mathbb{Q}(\sqrt{-D_2 N})$ is prime to p?

If instead of quadratic twists, one allows twists by Dirichlet characters of arbitrary order then a suggestion of Ralph Greenberg yields the following result.

Theorem 3.2. *Let K_1 and K_2 be imaginary quadratic fields and let S be a set of primes of Dirichlet density, $\delta(S) > 3/4$. Suppose that their class numbers satisfy*

$$h(K_1 L) \equiv 0 \pmod p \Leftrightarrow h(K_2 L) \equiv 0 \pmod p$$

for all cyclotomic extensions $L/\mathbb{Q}$ and for all $p \in S$. Then $K_1 = K_2$.

Proof. Suppose that $K_1 \neq K_2$. Let T be the set of (odd) primes in $\mathbb{Z}$ relatively prime to the class numbers $h(K_1)$, and $h(K_2)$, unramified in $K_1 K_2$, and with decomposition group equal to $\mathrm{Gal}(K_1 K_2/K_1) \subset \mathrm{Gal}(K_1 K_2/\mathbb{Q})$. Then T has density $\delta(T) = 1/4$. Since $\delta(S) > 3/4$, we must have $S \cap T \neq \emptyset$, and we can choose a prime $l \in S \cap T$. But any prime $l \in T$ splits in K_1 and is inert in K_2. It follows from Iwasawa theory (see [W, Chapter 13]) that the λ invariant for the cyclotomic $\mathbb{Z}_l$ extension of K_1 is at least one, whereas all the class numbers in the cyclotomic $\mathbb{Z}_l$ extension of K_2 are prime to l. It follows that $h(K_1 L_n) \equiv 0 \pmod l$ for some $n \geqslant 0$, and that $h(K_2 L_n)$ is prime to l for all $n \geqslant 0$, where L_n is the (unique) subfield of degree l^n of the cyclotomic field $\mathbb{Q}(\zeta_{l^{n+1}})$. This is a contradiction and hence $K_1 = K_2$. □

If we take a number field k in place of the rational field, $\mathbb{Q}$, then the set S must be taken sufficiently large in order to distinguish extensions of k by the class numbers of their twists as the following construction shows.

For any finite set S, there is a number field k such that the p-class tower is infinite for every prime $p \in S$ (see for example [Roq]). Then every finite extension L/k has class number $h(L)$, divisible by p, for every prime $p \in S$. For such a field, k, it is clear

that, given any two quadratic extensions K_1/k, and K_2/k, the class numbers $h(K_iL)$ are divisible by p for all $p\in S$, and all finite extensions L/k. In particular, $h(K_1(\chi))\equiv h(K_2(\chi))\equiv 0 \pmod p$ for all $p\in S$, and all (quadratic) characters χ.

4. L-functions of function fields over finite fields

Let $X/_{\mathbb{F}_q}$ be a complete, non-singular, projective curve of genus g defined over the finite field $\mathbb{F}_q$ and let $J(X)$ denote its Jacobian variety. If $K=K(X)$ is the function field of X, then K is a function field in one variable over $\mathbb{F}_q$. Let

$$L_X(T)=L_K(T)=\prod_{i=1}^{2g}(1-\alpha_iT)\in\mathbb{Z}[T]$$

be the numerator of the ζ-function of X (of K), so that the α_i are algebraic integers satisfying $\alpha_i\cdot\overline{\alpha_i}=q$. Let $K_n=\mathbb{F}_{q^n}\cdot K$ be the constant field extension of degree n of K so that the class number of $h(K_n)$ of K_n satisfies

$$h(K_n)=|J(X)(\mathbb{F}_{q^n})|=\prod_{i=1}^{2g}(1-\alpha_i^n).$$

Consider the situation of two such curves, X and X' defined over $\mathbb{F}_q$, with function fields K, and K' and Jacobians $J(X)$, and $J(X')$ respectively. We ask the analagous question to that considered in Section 3 for X, and X' viz.

Suppose that S is a set of primes, and that K and K' are two function fields over $\mathbb{F}_q$ such that for all $n\geqslant 1$ we have:

$$h(K_n)\equiv 0 \pmod p \Leftrightarrow h(K'_n)\equiv 0 \pmod p \text{ for all primes } p\in S.$$

then what can be said about L_K and $L_{K'}$?

Note that L_K is the characteristic polynomial of the Frobenius endomorphism acting on the l-adic Tate module of $J(X)$. In general, since the abelian varieties $J(X)$, and $J(X')$ may have the same simple factors but with differing multiplicities, we cannot expect that $L_K=L_{K'}$.

Theorem 4.1. *Let $\{\alpha_1,\alpha_2,\ldots,\alpha_t,\beta_1,\beta_2,\ldots,\beta_s\}$ be algebraic numbers, and let $R\geqslant 1$ be an integer. Suppose that*

$$\mathfrak{P}\mid\prod_{i=1}^{t}(1-\alpha_i^n)\Leftrightarrow\mathfrak{P}\mid\prod_{j=1}^{s}(1-\beta_j^n)$$

for all prime ideals $\mathfrak{P}\subset\bar{\mathbb{Q}}$ and for all $n\equiv 0 \pmod R$. Then for each integer $i, 1\leqslant i\leqslant t$, there exists an integer $j, 1\leqslant j\leqslant s$ and integers $N_i, N_j\in\mathbb{Z}$ such that

$$\alpha_i^{N_i}=\beta_j^{N_j}.$$

Proof. Let $E=\mathbb{Q}(\alpha_1,\alpha_2,\ldots,\alpha_t,\beta_1,\beta_2,\ldots,\beta_s)$ and let $|\boldsymbol{\mu}(E)|$ denote the order of the group of roots of unity in E. For each pair of indices $(i,j), 1\leqslant i\leqslant t, 1\leqslant j\leqslant s$, let $A_{ij}=\langle\alpha_i,\beta_j\rangle\subset E^\times$ be the multiplicative subgroup of E generated by α_i and β_j. Then $E^\times/A_{ij}$ has a *finite* torsion subgroup of order T_{ij} (say). Also, let T_i (respectively T_j) denote the order of the torsion subgroup of $E^\times/\langle\alpha_i\rangle$ (respectively $E^\times/\langle\beta_j\rangle$).

Fix an $\alpha_i\in\{\alpha_1,\ldots.\alpha_t\}$, and a prime $l>\max(T_i,T_j,T_{ij},|\boldsymbol{\mu}(E)|,R,s)$. Let ζ_l denote a primitive lth root of unity, and ζ_R a primitive Rth root of unity. Let $M=E(\zeta_l,\zeta_R,\alpha_i^{1/l})$, and $L=M(\beta_1^{1/l},\ldots,\beta_s^{1/l})$. Then L/M is a Kummer extension, of degree $[L:M]=l^r, r\leqslant s$, and with Galois group $\mathrm{Gal}(L/M)\simeq(\mathbb{Z}/l\mathbb{Z})^r$.

For each $j, 1\leqslant j\leqslant s$, let $L_j=M(\beta_j^{1/l})$ so that $M\subseteq L_j\subseteq L$, and let $H_j=\mathrm{Gal}(L/L_j)$.

Suppose that $\beta_j^{1/l}\notin M$ for all $j, 1\leqslant j\leqslant s$. Then $|H_j|=l^{r-1}$ for all $j, 1\leqslant j\leqslant s$, and so

$$\left|\bigcup_{j=1}^{s}H_j\right|\leqslant sl^{r-1}<l^r$$

since $l>s$. Therefore there exists $\sigma\in\mathrm{Gal}(L/M)$ but $\sigma\notin H_j$ for all $j, 1\leqslant j\leqslant s$. By Tchebatorev's density theorem, we may choose infinitely many prime ideals $\mathfrak{p}$ of M, relatively prime to l,α_i,β_j for all i, and j and such that $\mathfrak{p}$ is (totally) split for $M/\mathbb{Q}$ and such that the Artin symbol, $(\frac{L/M}{\mathfrak{p}})=\sigma_{\mathfrak{p}}=\sigma$. Completing at such a prime $\mathfrak{p}$, we see that $M_{\mathfrak{p}}\simeq\mathbb{Q}_p$, $p\equiv 1\pmod{lR}$ and that $\alpha_i^{1/l}\in\mathbb{Q}_p$. It then follows that $\alpha_i=x^l\in\mathbb{Q}_p$, so that $\alpha_i^{(p-1)/l}\equiv 1\,(\mathrm{mod}\mathfrak{p})$. On the other hand, by the choice of $\mathfrak{p}$, we see that $\beta_j^{1/l}\notin M_{\mathfrak{p}}$ for all $j, 1\leqslant j\leqslant s$, and therefore $\beta_j^{(p-1)/l}\not\equiv 1\,(\mathrm{mod}\mathfrak{p})$ for all j. But then we have $(p-1)/l\equiv 0\,(\mathrm{mod}\,R)$, $\mathfrak{p}|\prod_{i=1}^{t}(1-\alpha_i^{(p-1)/l})$ and $\mathfrak{p}\nmid\prod_{j=1}^{s}(1-\beta_j^{(p-1)/l})$. This contradicts the hypothesis of Theorem 3, and therefore we must have $\beta_j^{1/l}\in M=E(\zeta_l,\zeta_R,\alpha_i^{1/l})$ for some j.

Note that for an *abelian* extension M'/E', and for a prime l not dividing $|\boldsymbol{\mu}(E')|$, an element $x\in E'$ is an lth power in M' if and only if it is already an lth power in E' (see [Du–Ki] or [Sc]). By choice of the prime l, β_j is not an lth power in E, and so the above remark implies that β_j is not an lth power in $E(\zeta_l,\zeta_R)$. Therefore $E(\zeta_l,\zeta_R,\beta_j^{1/l})=E(\zeta_l,\zeta_R,\alpha_i^{1/l})$, and then Kummer theory implies that $\beta_j=\alpha_i^k x^l$ for some $x\in E(\zeta_l,\zeta_R)$ and some $k, 1\leqslant k\leqslant l-1$. But then β_j/α_i^k is an lth power in $E(\zeta_l,\zeta_R)$, and so also in E.

Now the group $A_{ij}=\langle\alpha_i,\beta_j\rangle$ is a two generator subgroup of $E^\times$, and therefore either $A_{ij}\simeq\mathbb{Z}\times\mathbb{Z}$ or $A_{ij}\simeq\mathbb{Z}\times(\text{finite})$ or $A_{ij}\subseteq\mu(E)$. If we had $A_{ij}\simeq\mathbb{Z}\times\mathbb{Z}$, then $A_{ij}/A_{ij}^l\simeq\mathbb{Z}/l\mathbb{Z}\times\mathbb{Z}/l\mathbb{Z}$. But by our choice of the prime l, $A_{ij}^l=A_{ij}\cap(E^\times)^l$, and since β_j/α_i^k is an lth power in E, it follows that $A_{ij}/A_{ij}^l\neq\mathbb{Z}/l\mathbb{Z}\times\mathbb{Z}/l\mathbb{Z}$. Hence there exist a $\gamma\in E^\times$, and a root of unity $\zeta\in\boldsymbol{\mu}(E)$, such that $\alpha_i=\gamma^{a_i}\zeta^{c_i}$ and $\beta_j=\gamma^{b_j}\zeta^{d_j}$ for some integers a_i,b_j,c_i and d_j. But then taking $N_i=b_j|\boldsymbol{\mu}(E)|$, and $N_j=a_i|\boldsymbol{\mu}(E)|$, we have $\alpha_i^{N_i}=\beta_j^{N_j}$. $\square$

We would like to point out that the case $t = 1 = s$ was proved by Corrales-Rodrigáñez and Schoof [Co–Sco] answering a question of Erdös. In fact, they were able to obtain the stronger result that $\alpha = \beta$ unless they were both roots of unity, or both were units with $\alpha = \beta^{-1}$. They also obtained an elliptic analogue of this result.

In general, however, one cannot expect such an improvement as the following example shows. If N and M are any positive integers, and ζ_N and ζ_M are primitive Nth, and Mth roots of unity respectively, then

$$\prod_{i=1}^{M} (1 - \zeta_M^i x^N) = \prod_{j=1}^{N} (1 - \zeta_N^j x^M) = 1 - x^{NM}.$$

If we take $\alpha_i = \zeta_M^i x^N$, and $\beta_j = \zeta_N^j x^M$, then the hypothesis of Theorem 4.1 is satisfied and we have $\alpha_i^M = \beta_j^N$, but smaller powers will not in general suffice.

Theorem 4.2. *Suppose that $R \geqslant 1$ is an integer, and that K and K' are two function fields over $\mathbb{F}_q$ such that for all $n \equiv 0 \pmod R$:*

$$h(K_n) \equiv 0 \pmod p \Leftrightarrow h(K'_n) \equiv 0 \pmod p \text{ for all primes } p.$$

Then there exists an integer N such that $L_{K_N}(T)$ and $L_{K'_N}(T)$ have the same zeros.

Proof. Let $h(K_n) = \prod_{i=1}^{2g}(1 - \alpha_i^n)$ and $h(K'_n) = \prod_{j=1}^{2g'}(1 - \beta_j^n)$. If $\mathfrak{P} \subset \bar{\mathbb{Q}}$ is any prime ideal dividing the rational prime p, then

$$\begin{aligned} \mathfrak{P} \mid \prod_{i=1}^{2g} (1 - \alpha_i^n) &\Leftrightarrow h(K_n) \equiv 0 \pmod p \\ &\Leftrightarrow h(K'_n) \equiv 0 \pmod p \\ &\Leftrightarrow \mathfrak{P} \mid \prod_{j=1}^{2g'} (1 - \beta_j^n). \end{aligned}$$

Applying Theorem 4.1, we see that for each integer $i, 1 \leqslant i \leqslant t$, there exists an integer $j, 1 \leqslant j \leqslant s$ and integers $N_i, N_j \in \mathbb{Z}$ such that $\alpha_i^{N_i} = \beta_j^{N_j}$. But since α_i, and β_j are both algebraic integers such that $|\alpha_i| = |\beta_j| = q > 1$, we must have $N_i = N_j$. Letting N be a common multiple of all the N_i we see that $L_{K_N}(T)$ and $L_{K'_N}(T)$ have the same zeros. □

Theorem 4.3. *Let A and B be abelian varieties defined over $\mathbb{F}_q$, simple over $\bar{\mathbb{F}}_q$, and let $R \geqslant 1$ be an integer. If for all integers $n \equiv 0 \pmod R$, and for all primes p,*

$$|A(\mathbb{F}_{q^n})| \equiv 0 \pmod p \Leftrightarrow |B(\mathbb{F}_{q^n})| \equiv 0 \pmod p,$$

then A and B are isogeneous over a finite extension of $\mathbb{F}_q$.

Proof. Let l be a prime number, relatively prime to q, and let $f_A(T)$, and $f_B(T)$ denote the characteristic polynomials of Frobenius acting on their respective l-adic Tate modules. Then we can write $f_A(T) = \prod_{i=1}^{2g_A}(1-\alpha_i T)$ and $f_B(T) = \prod_{j=1}^{2g_B}(1-\beta_j T)$ with

$$|A(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g_A}(1-\alpha_i^n)$$

and

$$|B(\mathbb{F}_{q^n})| = \prod_{j=1}^{2g_B}(1-\beta_j^n).$$

Theorem 4.1 then implies that there exists an integer N such that $f_{A,N}(T) = \prod_{i=1}^{2g_A}(1-\alpha_i^N T)$ and $f_{B,N}(T) = \prod_{j=1}^{2g_B}(1-\beta_j^N T)$ have the same zeroes. But then $f_{A,N}(T)$ divides $(f_{B,N}(T))^M$ for some integer $M \geqslant 1$, and so Tate's theorem [T] implies that A is $\mathbb{F}_{q^N}$-isogeneous to an abelian subvariety of B^M defined over $\mathbb{F}_{q^N}$. But since A and B were assumed to be simple over $\overline{\mathbb{F}}_q$, we see that A and B are isogenous over $\mathbb{F}_{q^N}$. □

Theorem 4.3 can be thought of as an analogue of Zarhin's conjecture over finite fields.

Ernst Kani has pointed out the following interesting instance of Theorem 4.2 in which only one prime (the characteristic) yields the result.

Let E and E' be elliptic curves defined over $\mathbb{F}_q$, and let K, and K' be their respective function fields. Suppose that E is supersingular and that $q = p^f$. Then since $h(K_n) = |E(\mathbb{F}_{q^n})|$ is prime to p for all n,

$$h(K_n) \equiv 0 \pmod{p} \Leftrightarrow h(K'_n) \equiv 0 \pmod{p}$$

implies that E' is also supersingular and then their ζ-functions become equal after an extension of degree at most 6.

5. Problems

We conclude this article with a number of questions which arising from the discussion of the previous sections. One can pose the following problems:

Question 1. Let S be a set of primes. Suppose that K_1 and K_2 are fields of degree $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = d$. Suppose that for every (cyclotomic) extension $L/\mathbb{Q}$, the class

numbers $h(K_iL)$ satisfy:

$$h(K_1L) \equiv 0 \pmod{p} \Leftrightarrow h(K_2L) \equiv 0 \pmod{p} \text{ for all } p \in S.$$

If S is sufficiently large (e.g. S is the set of all primes), does this imply that $K_1 = K_2$? Since we think of the class number as the algebraic part of an L-function at the critical point $s = 1$, we can also pose the analagous question at other critical points. Appealing to Lichtenbaum's conjecture [Li, Question 4.2], we can replace the class numbers by the orders of the K-groups $K_{2n}(\mathcal{O}_{K_iL})$ and again ask if the prime factors of these group orders characterize the fields K_i as L ranges over all finite (cyclotomic) extensions of $\mathbb{Q}$. (Here $\mathcal{O}_{K_iL}$ denotes the ring of integers in the number field K_iL).

Question 2. If we replace the Dedekind ζ-functions by the ζ-functions of curves (varieties) over finite fields, we can ask for analogues at of Theorems 4.1 and 4.2 at other values of s. Given $0, 1 \neq r \in \mathbb{Q}$, and a (sufficiently large) set I of integers n, and a set S of primes, suppose that

$$\prod_{i=1}^{t} (r - \alpha_i^n) \equiv 0 \pmod{p} \Leftrightarrow \prod_{j=1}^{s} (r - \beta_j^n) \equiv 0 \pmod{p} \text{ for all primes } p \in S$$

for all $n \in I$, and all $p \in S$. What conditions on I and S allow us to conclude that $\{\alpha_1, \alpha_2, \ldots, \alpha_t\} = \{\beta_1, \beta_2, \ldots, \beta_s\}$?

As an example, the following problem of elementary number theory is a special case (taking $s = t = 1$ above):

If A and B are positive integers such that for all primes p, and all integers $n \geqslant 1$,

$$p | A^n - 2 \Leftrightarrow p | B^n - 2,$$

does this imply that $A = B$?

We prove this assuming the ABC conjecture.

The ABC conjecture asserts that given coprime positive integers A, B, C with $A + B = C$ then for any $\varepsilon > 0$, there is a constant $c(\varepsilon) > 0$, such that $C < c(\varepsilon)\mathrm{rad}(ABC)^{1+\varepsilon}$, where for a positive integer N, $\mathrm{rad}(N) = \prod_{p|N} p$ is the product of the distinct prime factors of N. We will say that the sequence $\{N_n\}$ has *finite support* if the sequence $\mathrm{rad}(N_n)$ is bounded. Otherwise, we say that $\{N_n\}$ has *infinite support*.

Lemma 5.1. *Assume the ABC conjecture. Let a, N be positive integers. Then an infinite subsequence of the integers $aN^n + b$ has finite support if and only if either $N = 1$, or $b = 0$.*

Proof. Clearly if either $N = 1$, or $b = 0$, then $aN^n + b$ has finite support.

Suppose that there is some infinite set of integers I, and some bound $M>0$, such that $\mathrm{rad}(aN^n+b)\leqslant M$ for all $n\in I$. Take $A=aN^n, B=b$, and $C=aN^n+b$. Then the ABC conjecture (after adjusting for common factors) implies that given $\varepsilon>0$, there is a constant $c(\varepsilon)$ such that if $ABC\neq 0$

$$aN^n+b\leqslant c(\varepsilon)(\mathrm{rad}(ABC))^{1+\varepsilon}\leqslant c(\varepsilon)(abNM)^{1+\varepsilon}$$

for all $n\in I$. But then $N^{n-1-\varepsilon}$ is bounded, and since n is unbounded, we must have $N=1$. □

Proposition 5.2. *Assume the ABC conjecture. Let $a>0, b, c>0, d\in\mathbb{Z}$ be integers. Suppose that A and B are positive integers such that*

$$p\mid aA^n+b\Leftrightarrow p\mid cB^n+d$$

for all primes p and for an infinite sequence I of positive integers n. Then either both of the sequences aA^n+b and cB^n+d have finite support, or $A=B$ and $d(aA^n+b)=b(cB^n+d)$.

Proof. It is clear that the hypothesis implies that one of the sequences has finite support if and only if the other does. Therefore we may assume that they both have infinite support. If $bd=0$ then one and hence both of the sequences are finitely supported. Hence we may assume that $abcd\neq 0$.

Suppose that $A<B$, and choose ε so that $A^{1+\varepsilon}<B$. Consider the equation

$$(cB^n+d)-d=cB^n.$$

Then the ABC conjecture (after removing common factors) implies that there is a constant $c(\varepsilon)$ independent of n such that

$$B^n\leqslant c(\varepsilon)(\mathrm{rad}(cBd(cB^n+d)))^{(1+\varepsilon)}.$$

But $\mathrm{rad}(cB^n+d)=\mathrm{rad}(aA^n+b)\leqslant 2aA^n$ for n large and therefore

$$B^n\leqslant c(\varepsilon)(|cBd2a|A|^n)^{(1+\varepsilon)}.$$

Taking nth roots and letting $n\to\infty$, we obtain $B\leqslant A^{(1+\varepsilon)}$. But this is a contradiction, and therefore $A=B$.

Thus we have

$$p\mid aA^n+b\Leftrightarrow p|cA^n+d$$

for an infinite set of exponents n. But for any prime p, with $p|aA^n+b$ it follows that $p|ad-bc$, and since we assumed that the sequence $\{aA^n+b\}$ had infinite support, Lemma 1 implies that $ad=bc$. Therefore $d(aA^n+b)=b(cB^n+d)$. □

Hence we have the following:

Corollary 5.3. *Assume the ABC conjecture. Suppose that A and B are positive integers such that*

$$\mathrm{rad}(A^n - 2) = \mathrm{rad}(B^n - 2),$$

for an infinite sequence of integers n, then A = B.

References

[An–Ch] N.C. Ankeny, S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. 5 (1955) 321–324.

[B–C–D–Ta] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001) 843–939.

[Co–Sco] C. Corrales–Rodrigáñez, R. Schoof, The support problem and its elliptic analogue, J. Number Theory 64 (2) (1997) 276–290.

[Du–Ki] D. Dummit, H. Kisilevsky, Abelian extensions generated by division points, J. Number Theory 29 (1) (1988) 21–30.

[Fr–Ho] S. Friedberg, J. Hoffstein, Nonvanishing theorems for automorphic L-functions on $GL(2)$, Ann. Math. 142 (1995) 385–423.

[Ha] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, J. Number Theory 6 (1974) 276–278.

[Jo] N. Jochnowitz, Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves, preprint, 61pp.

[Ki] H. Kisilevsky, Rank determines semi-stable conductor, J. Number Theory, to appear (doi: 10.1016/S0022-314X(03)00157-4).

[Li] S. Lichtenbaum, Values of zeta functions, étale cohomology, and algebraic K-theory, in: H. Bass (Ed.) Algebraic K-theory II, Lecture Notes in Mathematics, Vol. 342, Springer, Berlin, 1973, pp. 489–501.

[Mi] T. Miyake, Modular Forms, Springer, New York, 1989.

[Na] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd Edition, Springer and PWN–Polish Scientific Publishers, New York and Warsaw, 1990.

[O–Sk] K. Ono, C. Skinner, Fourier coefficients of half-integral weight modular forms modulo, Ann. Math. (2) 147 (1998) 453–470 Corrigendum: Ann. Math. (2) 148 (1998) 361.

[O–Sk2] K. Ono, C. Skinner, Non-vanishing of quadratic twists of modular L-functions, Invent. Math. 134 (1998) 651–660.

[Ro] D. Rohrlich, The vanishing of certain Rankin–Selberg convolutions, in: R. Murty (Ed.) Automorphic Forms and Analytic Number Theory, Univ. Montréal, Montréal, Que., 1989, pp. 123–133.

[Roq] P. Roquet, On class field towers, in: J.W.S. Cassels, A. Frölich (Eds.) Algebraic Number Theory, Brighton 1965, Academic Press, New York, 1967, pp. 231–249.

[Sc] A. Schinzel, Abelian polynomials, power residues and exponential congruences, Acta Arith. 32 (1977) 245–274.

[Sh] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Iwanami Shoten, Japan and Princeton University Press, Princeton, NJ, 1971.

[T] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.

[Ta–Wi] R. Taylor, A. Wiles, Ring–theoretic properties of certain Hecke algebras, Ann. Math. (2) 141 (3) (1995) 553–572.

[W] L. Washington, Introduction to Cyclotomic Fields, Springer, New York, 1982.
[Wa] J. Waldspurger, Sur les valeurs de certaines fonctions L automorphe en leur centre de symétrie, Comp. Math. 54 (1985) 173–242.
[Wi] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. Math. (2) 141 (3) (1995) 443–551.